MAYO - JUNIO 2015

iT ahora





Rubén
Recalde

CIO

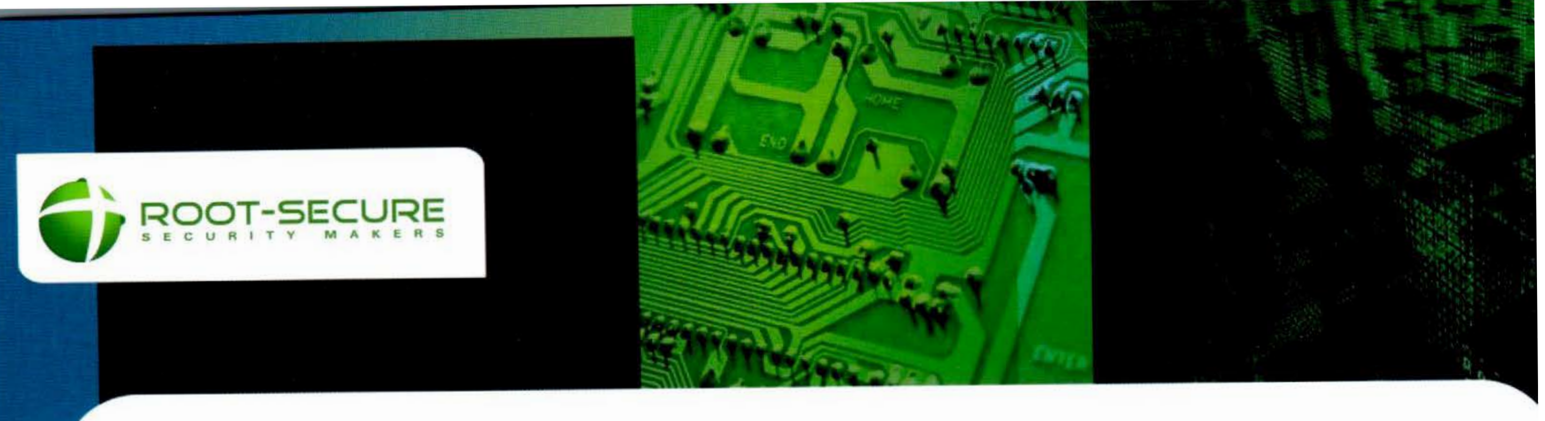
PRONACA



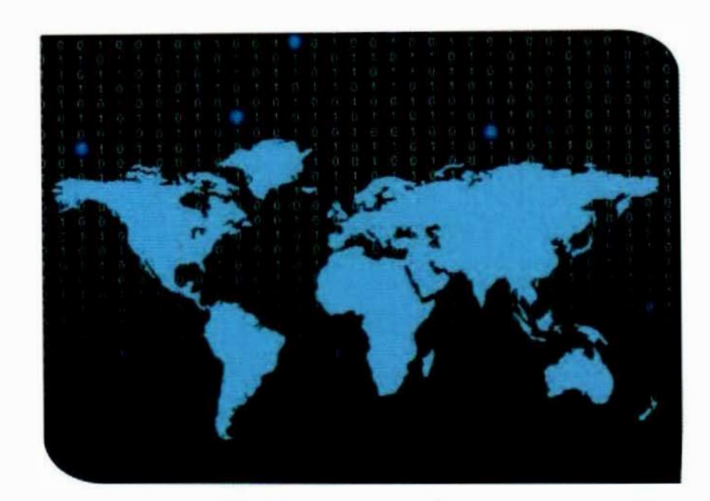


3000 ejemplares

SEGURIDAD • CLOUD • COMPUTING • BIG DATA • SOFTWARE • BI



ISO 27000
¿NECESIDAD, OBLIGACIÓN O MODA?



ISO 27000

Te da una visión parcial acerca de los beneficios que puede aportar a las organizaciones una certificación de este estilo, ISO 27000 se trata de un "Marco de Referencia" sobre el cual se debe trabajar, y no de un esquema rígido a ser implementado por las compañías.

La familia de las ISO

- ISO 27001
- ISO 27002
- ISO 27003
- ISO 27004
- ISO 27005
- ISO 27006

Nuestro objetivo

Gestionanar adecuadamente la Seguridad de su Información.

Nuestro servicio

Temas específicos incluidos en cualquiera de las ISO 27000, recomendamos los aspectos fundamentales relacionados con un Sistema de Gestión de Seguridad de la Información, partiendo de una política que contemple:

1. El compromiso de la alta dirección, interviniendo en el tema por lo menos una vez al año.
2. Un Comité de Seguridad de la Información, responsable por la implementación de las medidas que la empresa considera adecuadas, que reporte a la Dirección.
3. La asignación de roles y responsabilidades que conforman la estructura organizacional.
  a. Oficial de Seguridad (CSO).
  b. Dueños de Datos.
  c. Administradores de Seguridad.

Beneficios esperables

Medir los dos aspectos básicos
que hacen a la Seguridad de la Información:

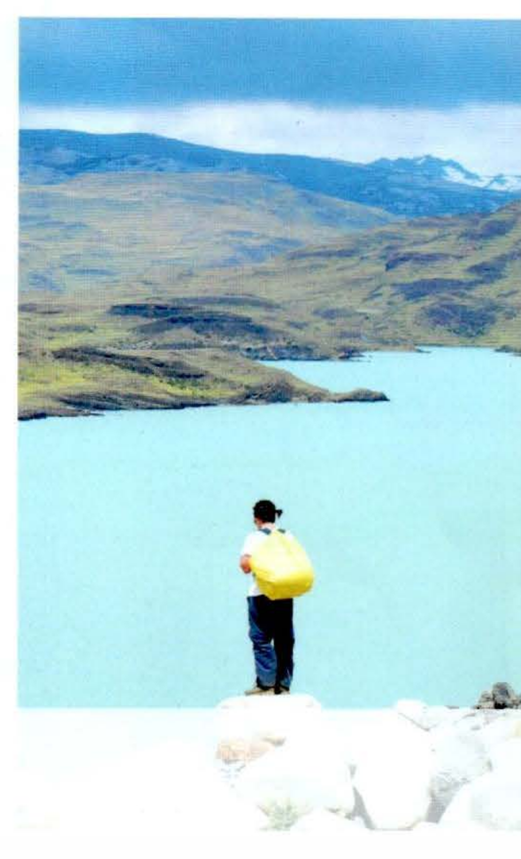
1. Si existe un Sistema de Gestión de Seguridad de la Información
  a. Por medio de la revisión de la Alta Dirección.
  b. La implementación y seguimiento de planes por el Comité.

2. La implementación de controles específicos por medio del cumplimiento de las normas.













Seguridad

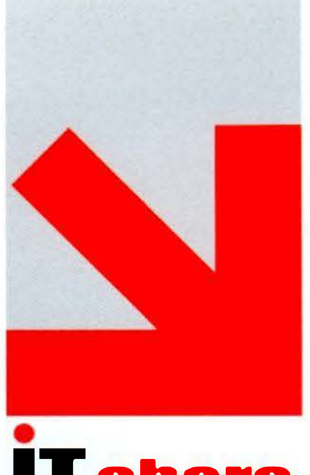
¿QUÉ HACEMOS?

Protegemos la información y la infraestructura que la soporta de tal manera de garantizar su disponibilidad, integridad y confidencialidad.

SOLUCIÓN

Disponemos de tecnologías de última generación que permiten proteger los perímetros, las plataformas internas, los dispositivos móviles y los procesos de negocios, todo ellos con plataformas de correlación de eventos de seguridad monitoreados por nuestro Security Operation Center (SOC).

IT Ahora: Un nuevo reto



IT ahora

Directora
Janeth Martinez
janeth.martinez@itahora.com

Editora
Anavela Herrera
anavela.herrera@itahora.com

Diseño y Diagramación
Cristina Orellana
crisoreog@gmail.com

Fotografía
Innovacom
Portada: Xavier Jácome

Colaboraciones
Germán Pancho
Diego May

Marketing y Comercialización
Fernando Carvajal

Corrección de estilo
Innovacom

Asistente
Jésica Fernández

Contadora
Elizabeth Erazo

No importa cuán rápido adoptemos la tecnología ni qué tan integrados tengamos los ejes de innovación a nuestras empresas si detrás de eso no están las personas persiguiendo un objetivo que –primero- es individual, de carrera, de realización personal. No hay tecnología sin personas. Ese es el principio que anima esta nueva etapa de IT Ahora y que ponemos en sus manos.

En un mundo cambiante y vertiginoso impuesto por la tecnología, nuestra propuesta es destacar y rescatar a todos los protagonistas que actúan, lideran, disfrutan, gestionan, crean, consumen, desarrollan, promueven y participan de este gran ecosistema que son las Tecnologías de la Información y Comunicación.

Nuestro principio es que detrás de una decisión siempre está un ser humano poniendo en juego sus conocimientos, pensamientos, creatividad y sus valores para que el proyecto consiga eso que todos buscamos: terminar nuestras jornadas de trabajo con una sonrisa de satisfacción; con una historia que contar al llegar a casa o simplemente con la alegria de una tarea cumplida.

A esas personas que hacen la diferencia les dedicamos esta edición y las que vendrán. Estamos convencidos de que si nos sentamos frente a una taza de café con la grabadora encendida encontraremos a personajes dignos de admiración; a equipos motivados y a empresas exitosas. Llevamos más de 20 años encontrando esas historias en el mundo de la tecnologia y también poniendo a sus órdenes nuestra vocación de ser los oidos y los medios para comunicar.

Anavela Herrera

El compromiso de IT Ahora es escuchar las necesidades de nuestros lectores que son usuarios empresariales del sector privado y público, que tienen la responsabilidad de definir políticas para un buen gobierno corporativo e implementar soluciones ajustadas a los cambios del negocio.

Desde esta edición, IT Ahora da un giro para entregar información actualizada de soluciones disponibles en el país, inspirar al emprendimiento, analizar desde distintos puntos de vista las tendencias tecnológicas, y además, entretener a nuestros lectores.

Rubén Recalde, nuestro primer perfil de portada, deja por un momento de ser el ejecutivo de la empresa Top 10 del país para permitirnos conocer al ser humano tenaz, metódico y profundamente agradecido con la vida.

En la misma línea de convicción está el emprendimiento con base tecnológica; para nosotros es un eje importante en el desarrollo económico del pais, de manera que es nuestra responsabilidad, en esta y futuras publicaciones, incentivar a las empresas a apoyar esas geniales ideas que nacen del entorno y en particular de sus propios colaboradores.

Esperamos disfruten de esta publicación como nosotros lo hicimos y les invitamos a participar en nuestros espacios de Opinión.

Finalmente, queremos agradecer a quienes confian y apoyan este proyecto. Apreciamos sobremanera esas palabras de aliento que hemos escuchado durante estas semanas. Si contamos con su favor, ese "¡Les va a ir muy bien!" se hará realidad.

Janeth Martínez

Comentarios o sugerencias escríbanos a redaccion1@itahora.com

IT Ahora es una revista ecuatoriana que en cumplimiento con los requisitos promulgados por la nueva Ley de Comunicación vigente en la República del Ecuador, pone en conocimiento público a través de la revista y nuestra página web www.itahora.com nuestra políticas editoriales e informativas como visión y misión. Somos una revista apta para todo público que se distribuye a nivel nacional.

IDENTIFICA NUESTROS CONTENIDOS BAJO ESTA ICONOGRAFÍA:

I Informativo · O Opinión · P Publicitario · F Formativo / Educativo · E Entretenimiento · D Deportivo

Imprima las tarjetas de sus clientes o empresa de forma instantánea



Y optimice los procesos dentro de su compañía gracias a la **Serie ZXP** Impresoras de tarjetas de Zebra



8

7

3

3 Impresora ZXP3

Confiable y fácil de usar, la ZXP Serie 3 es todo lo que puede desear en una impresora de tarjeta profesional . La ZXP Serie 3 es una solución ideal para aplicaciones de impresión individuales o de doble cara de bajo a mediano volumen que requieren una formación mínima del operador y una excelente calidad de impresión. ZXP Series 3 impresoras ofrecen funciones avanzadas y opciones de medios de alta capacidad.

7 Impresora ZXP7

Tiene excelente impresión de tarjetas de calidad fotográfica en medio y aplicaciones de gran volumen . La ZXP Serie 7 ofrece un rendimiento aún rápido y confiable al tiempo que ofrece a los usuarios un valor excepcional al reducir el coste total de la impresora de la propiedad . Una y otra vez, imprime afilados tarjetas vívidas con control del color preciso.

8 Impresora ZXP8

Con la innovadora línea de impresoras de tarjetas 8 retransferencia ZXP Series de Zebra, crear colores vivos y las tarjetas en blanco y negro bajo demanda con calidad de imagen de ensueño.

Dsitrbuidor Autorizado para Ecuador:

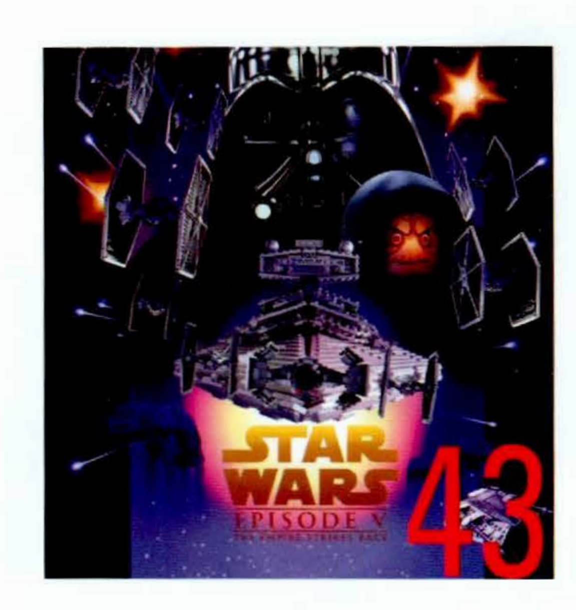


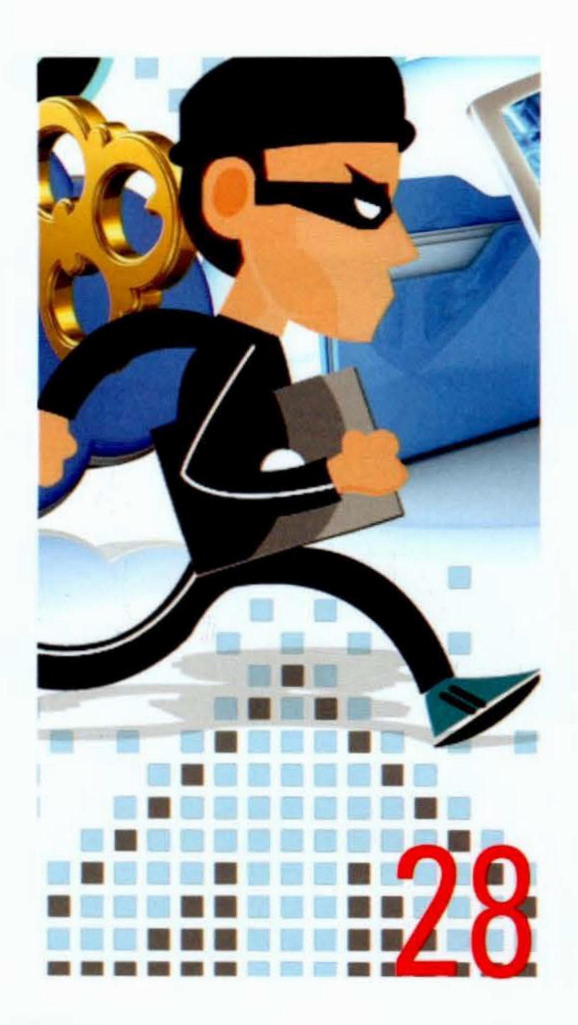
SUMARIO





SEGURIDAD







Oficina de Manejo y Gestión de Proyectos.



Nuestros servicios de PMO permiten llevar el control de sus proyectos de inicio a fin usando metodología PMI adaptada a sus necesidades con el fin de garantizar los resultados deseados en cualquier campo, sea este ingeniería, tecnología, construcción, procura de elementos, etc.

Todos nuestros servicios y proyectos son administrados desde una PMO (Project Management Office) en la cual contamos con consultores certificados como PMP's. La experiencia acumulada de años y decenas de proyectos administrados, nos permite brindar este servicio a nuestros clientes, siguiendo estándares definidos en buenas prácticas como las del Project Management Institute.

Creemos que todo problema en la vida puede ser resuelto de una forma creativa y nuestra pasión es encontrarla!

www.kruger.com.ec | info@kruger.com.ec | Tel: 593 2 383 0050





IBM y Facebook anunciaron alianza



Facebook e IBM Commerce trabajarán juntos combinando las tecnologias de anuncios de Facebook con IBM Journey Analytics, de manera que se pueda determinar adecuadamente qué grupos de consumidores se encuentran activos en Facebook y establecer correlaciones entre sus intereses e interacciones entre múltiples canales. La información que esto arroja puede luego ser aplicada a la solución Journey Designer de IBM para servir como guía en la entrega acertada de mensajes adecuados para los consumidores finales de cada marca.

IBM también anunció que Facebook será el primer socio que se incorporará al nuevo IBM Commerce THINKLab, un entorno de investigación y colaboración en el que las compañías trabajarán directamente con las marcas para acelerar el desarrollo de nuevas tecnologías diseñadas para personalizar la experiencia del cliente.

Deloitte presentó aplicación digital

Deloitte Ecuador creó un canal dinámico de comunicación con sus clientes a través de una herramienta que permite conocer en tiempo real las últimas novedades e información relevante sobre las Normas Internacionales de Información Financiera, NIIFs.

La aplicación desarrollada por profesionales ecuatorianos fue diseñada para todos los usuarios que requieran conocer las últimas novedades legales, tendencias, información actualizada sobre NIIFS, así como acceder a sus obligaciones tributarias de manera calendarizada a fin de cumplir con todas y cada una de ellas.

Son seis las secciones que los usuarios podrán revisar en la aplicación:

NIFFs News.- corresponde a un conjunto único de normas, legalmente exigibles y globalmente aceptadas, basados en principios que requieren que los estados financieros contengan información comparable, transparente y de alta calidad.

Audit News.- publicación de boletines de temas tecnológicos donde los usuarios conocerán a fondo sobre las últimas novedades en seguridades y manejo de la información.

Registros Oficiales.- Con resúmenes de las principales leyes, decretos, resoluciones y acuerdos publicados en el Registro Oficial durante todos los meses del año. Calendario Tributario.- Los usuarios pueden administrar sus obligaciones tributarias con tan solo incluir su número de cédula o RUC, tendrán notificaciones de las fechas en las cuales deben realizar su planificación y un detalle del concepto de las mismas.

Tendencias.- Consta de artículos y estudios de temas gerenciales de actualidad. Novedades Legales.- Consiste en una publicación mensual en la cual se encuentran las últimas novedades legales y tributarias.

Adexus presentó el "Adexus Cloud Services"



Adexus Ecuador realizó el Lanzamiento de Adexus Cloud Services y la presentación de los Servicios de recuperación de desastres para ambientes virtualizados, Oferta de Servicios SAP, Big Data y Cisco Cloud Innovations.

En la foto están: Jasson Boada, gerente Comercial Nacional Adexus Ecuador; Manuel Lapo, Country Manager Adexus Ecuador; Víctor Palma, gerente de OperacionesAdexus Chile; Eduardo Guzmán subgerente de Gestión Técnica Gerencia de Operaciones CGSI Adexus Chile y Alejandro Silva, subgerente de Arquitectura y Productos Centro de Datos Adexus Chile.

Automatizamos procesos para **optimizar** recursos





Facturación electrónica
Para su empresa



Importantes descuentos todo 2014 por aniversario

30% Hasta Agosto
20% Hasta Octubre
10% Hasta Diciembre



Completo conjunto de soluciones en

- **Finanzas**
  - Compras
  - Ventas
  - Cuentas por cobrar
  - Cuentas por pagar
  - Contabilidad
  - SRI
  - Facturación electrónica Integrada
- **Activos fijos**
  - Depreciación automática
  - Registro contable
  - Ficha de depreciación por cada activo
- **Logística**
  - Bodegas
  - Preventa
  - Auto venta
  - Distribución
- **Abastecimiento**
  - Requisiciones de compra
  - Gestión de compras
  - Órdenes de compra (OC)
  - Ingresos a bodega de las OC
- **Producción**
  - Análisis de costos unitarios
  - Recetas de producción
  - Ordenes de producción (OP)
  - Requisición de recursos
  - Imputación de costos
  - Liquidación de OP
- **Business Intelligent**
  - Cubos comerciales
  - Cubos de cartera
  - Cubos logísticos
  - Cubos de producción
  - Cubos financieros

¿Por que NEURAL?

- Potente
- Rápido
- Confiable
- Integrado
- Probado
- Seguro

Telf.: 02-602 5342 / 02-245 4843
Dir: Japón y Agustín Gerrero Esq. Ed. Torres Japón Of. 703E
www.neural.com.ec / mail: info@neural.com.ec • Quito - Ecuador



1 de cada 4 empresas ecuatorianas clasifica su información crítica

Las tendencias de seguridad señalan que el robo de información, uso de vulnerabilidades de sistemas y la ingeniería social serán las más utilizadas por los ciberdelincuentes en el 2015 y las actividades de concientización en las empresas apenas alcanzan el 40% en Latinoamérica, así lo indicó Maximiliano Cantis, gerente de Canal de ESET para Centroamérica y norte de Sudamérica, durante el Security Day de ESET realizado en Quito.

Entre otras cifras, Cantis señaló que en Ecuador solamente 1 de cada 5 empresas cuenta con una solución de back up para contrarrestar las amenazas de virus como Randsomware, un programa malicioso que bloquea los datos del usuario y los activa a cambio de un pago.

El entorno de seguridad exige que se combine tecnología, acciones para mejorar la seguridad y personal responsable del área.

Para Cantis, la seguridad informática es la subdivisión más importante y más vinculada al negocio de manera que la inversión debería ser proporcional y en función de los activos digitales de la corporación.

Aunque se recomienda que las empresas clasifiquen la información crítica del negocio, solamente 1 de cada 4 empresas ecuatorianas lo hace.

Al referirse a la seguridad de la información cuando las empresas adoptan el ecosistema cloud, Cantis sostuvo que, no porque la información está en la nube, la inversión en seguridad es mayor. "Hay que entender qué parte de mi operación digital del negocio está en la nube y, una vez definida, se procede a tomar acciones pertinentes de seguridad", indicó el ejecutivo de ESET



Maximiliano Cantis, gerente de Canal de ESET para Centroamérica y norte de Sudamérica

APARECE UNA NUEVA FIGURA EN EL DIRECTORIO: EL CISO

El valor que tiene la información digital del negocio exige a las empresas considerar dentro de su departamento de tecnología a un profesional con experiencia y especializado en seguridad; este profesional al que se le asignado como un CISO (Chief Information Security Officer) está en relación directa con el gerente, y muchas veces no depende del CIO.

Este profesional tiene la función de entender el negocio y la información clave que debe cuidar, además, coordinar acciones directamente con el gerente general y proyectar presupuestos y asignaciones para seguridad.

A su vez, en pequeñas y medianas empresas, las funciones de este CISO las asume el gerente de sistemas, comenta Canttis.



ICAAN realiza actividades de concientización en la región

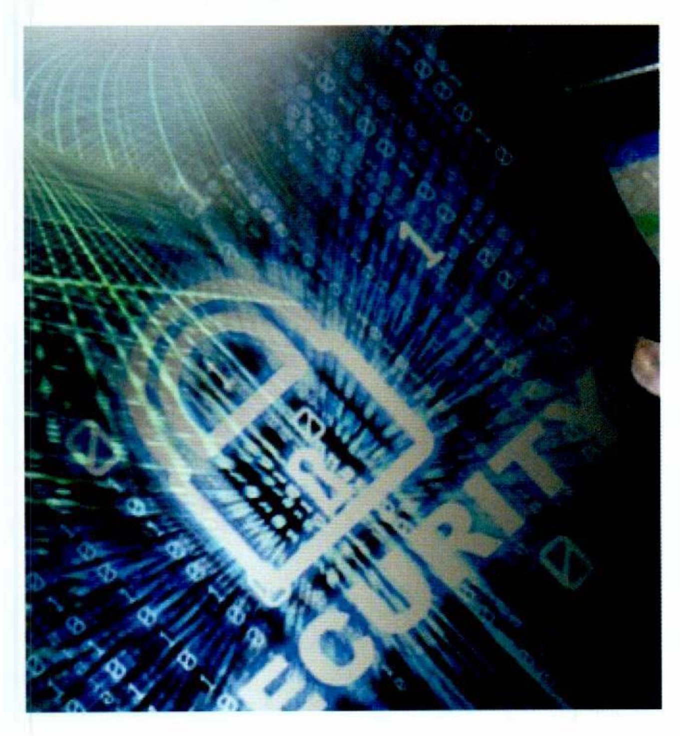
La Corporación de Internet para la Asignación de Nombres y Números, ICANN (siglas en inglés), lleva a cabo una serie de proyectos para los diferentes grupos de interés de América Latina y el Caribe dentro de su Plan Estratégico Regional.

El objetivo es la difusión de los principales desafíos que afronta la región en relación a Internet, su gobernanza y administración.

Una de las actividades es el Roadshow realizado en la región Andina con el fin de difundir las novedades sobre el programa global de Dominios Genéricos de Alto Nivel (gTLD) y la transición al Protocolo de Internet versión 6 (IPv6).

La importancia de estas novedades radica en los nuevos usos que posibilita la ampliación del programa global de Dominios Genéricos de Alto Nivel (o gTLD por sus siglas en inglés) por la cual aumenta la cantidad de dominios disponibles para ser utilizados (de 22 a más de 1300). De esta manera, las empresas y comunidades tienen la posibilidad de elegir su propio nombre de dominio para diferenciarse y así volverse más competitivos.

Otro de los tópicos sobre el cual la comunidad regional se encuentra trabajando está relacionado a la vulnerabilidad de Internet y la nueva tecnología llamada DNSSEC, desarrollada para brindar protección contra ataques desde el primer paso del proceso de búsqueda y certificar la validez de la dirección del sitio que se está visitando.





HP presentó sistema de configuración virtual

Para los directores o administradores de TI, es importante contar con la información necesaria sobre su infraestructura para la toma de decisiones, y para ello, HP a través de Compuequip DOS presentó una herramienta de configuración virtual para la revisión de los componentes de infraestructura.
Cristian Pasquel, gerente de Producto HP de Compuequip DOS, señaló que el sistema de configuración virtual permitirá presentar de manera visual la infraestructura que adquiere el cliente, además, de las necesidades presentes y a futuro, por ejemplo, respecto a espacio de almacenamiento.
Durante la presentación, se realizó una demostración para un sistema de almacenamiento y se analizó el espacio que puede utilizar una empresa y sus requerimientos de discos según la previsión de su crecimiento.
Esta herramienta será de ayuda para que los gerentes de TI conozcan al detalle sobre sus conexiones, cables, procesadores, así como el consumo de espacio en el data center, etc.
Pasquel comenta que el sistema de simulación convergente posibilita al cliente tomar decisiones más rápidamente en cuanto a sus presupuestos futuros de crecimiento.



Desde la tecnología UHF a tecnología satelital

La tecnología de rastreo, ubicación y recuperación de vehículos ha pasado distintas fases y uso de herramientas. En 21 años, la empresa Carseg, empresa especializada en monitoreo y soluciones de seguridad para vehículos, ha utilizado tecnología UHF, satelital, RDFI, GPS para desarrollar productos de seguridad física de automóviles, flotas, etc.
Guido Jalil, director de Carseg, indicó que la tecnología de ondas de radio fue la primera que se incorporó a través de productos LoJack, aunque con el tiempo se empezó a utilizar dispositivos más pequeños, poderosos y con un consumo eficiente de energía.
La tecnología GPS abrió oportunidades de desarrollar productos, aunque al inicio era una tecnología costosa. Comenta que la tecnología GPS se utilizó con la banda de celulares CDMA con las limitaciones del caso, cobertura limitada y una dispersión de ubicación de los vehículos de hasta 300 metros.

Los adelantos tecnológicos están facilitando la interacción con el cliente, ahora es factible el seguimiento remoto de los vehículos a través de la computadora e inclusive de aplicaciones para celulares.
En estos cambios tecnológicos, lo que se ha incrementado son las acciones que se pueden realizar con el automóvil, desde encenderlo o apagarlo, escuchar conversaciones en el vehículo, es decir acciones que van más allá del robo de vehículos, comenta Jalil.
Además, sostiene que la tecnología de transmisión satelital es un recurso que a futuro y, gracias a la reducción de costos y una mejor cobertura, se convertirá en una tecnología para innovar y presentar soluciones de geolocalización, seguridad y logística.



Guido Jalil, director de Carseg

M2MONEY & PAYMENTS LATAM 2015 9na Edición

29 Y 30 DE JULIO | QUITO, ECUADOR | JW MARRIOTT

YA LLEGÓ LA BILLETERA ELECTRÓNICA A ECUADOR Y AMÉRICA LATINA

ALGUNOS ORADORES CONFIRMADOS:

- **ROSANNA RAMOS VELITA,** Chairman of the Board, Caja Rural los Andes.
- **JORGE MONCAYO,** Inclusión Financiera, Banco Central del Ecuador.
- **FAUSTO RICARDO VALENCIA BATALLAS,** Director del Proyecto del Dinero Electrónico, Banco Central del Ecuador.
- **Representante de Better Than Cash Alliance**
- **CARLOS MELEGATTI,** Director, Banco Central de Costa Rica.
- **ELIZABETH McQUERRY,** Ph.D, Glenbrook Partners.
- **FERNANDO D´ALESSIO,** Cofundador, Linio.
- **MIREYA ALMAZÁN,** Mobile, Money for the Unbanked, GSMA.
- **ANDRÉS BUBANO DE LARA,** Presidente, Directorio Asociación Ecuatoriana de Software.

!Aproveche los precios rebajados disponibles para los miembros de AESOFT y la Cámara de Comercio de Quito!

PARA DIRECTIVOS DE:

- OPERADORAS MÓVILES
- RETAILERS
- MAYORISTAS
- COOPERATIVAS
- BANCOS
- EMISORES
- INSTITUCIONES FINANCIERAS

3ra Edición

M2PAYMENTS AWARDS LATAM

LA PREMIACIÓN DISTINGUE LAS INICIATIVAS DE DINERO MÓVIL MÁS INNOVADORAS DE LATINOAMÉRICA

ASISTA A LA CEREMONIA EL DÍA 29 DE JULIO

ALGUNOS TEMAS A TRATARSE

- MONETIZANDO EL DINERO MÓVIL CON MODELOS DE NEGOCIOS SÓLIDOS CON APLICACIONES MÓVILES
- CASO DE ESTUDIOS DE DINERO MÓVIL EN LATINOAMÉRICA: "MONEDERO MÓVIL" EN COSTA RICA Y "TIGO CASH" EN PARAGUAY
- CONOZCA CUÁLES BANCOS Y OPERADORES ESTÁN LIDERANDO LAS TENDENCIAS EN LA IMPLEMENTACIÓN DE LA TECNOLOGÍA NFC
- DINERO ELECTRÓNICO EN EL ECUADOR LUEGO DEL LANZAMIENTO DEL PILOTO
- EVOLUCIONANDO EN EL MERCADO DE LOS PAGOS MÓVILES Y EL COMERCIO ELECTRÓNICO

APOYAN









IDNoticias






FrecuenciaEVENTS

¡PARA PATROCINIOS Y ASISTENCIA CONTÁCTENOS AHORA!



Buenos Aires +54911 5872-5872

Quito 593.2.3300907
0998385557

La seguridad analizada desde el Infosecurity

La XI edición del Infosecurity 2015 de Quito se desarrolló en abril y contó con la asistencia de expositores, firmas de seguridad y alrededor de 350 ejecutivos: directores, gerentes y administradores de Tecnologías de Información y de Seguridad. Infosecurity es el evento que durante cuatro meses recorre 24 ciudades de Latinoamérica y el Caribe y enfoca los principales temas de tendencias sobre seguridad.

En una agenda amplia de conferencistas se dictaron temas sobre auditoría y protección de datos; ciberseguridad inteligente; seguridad y ciberguerra: estrategia de continuidad del negocio; tendencias de seguridad; protección contra amenazas adaptativas, etc.



LAS EMPRESAS DEBEN VELAR POR LA SEGURIDAD INTERNA

Innovasys, compañía ecuatoriana con experiencia en soluciones tecnológica, a través de su experiencia en el análisis estadístico, ha definido que en Ecuador se presta atención de seguridad perimetral sin embargo, se descuida la seguridad interna, así lo señaló Fernanda López, gerente Comercial de Innovasys.


Gastón Pavez,
Unidad de Negocios de IBM Security

LA SEGURIDAD TAMBIÉN UTILIZA HERRAMIENTAS DE INTELIGENCIA

En Infosecurity, un protagonista fue el impacto de la seguridad en las compañías y el cambio de paradigma de los cibercriminales que investigan, analizan y utilizan ingeniería social y tecnología sofisticada para sustraer información. De allí que para Gastón Pavez, de la unidad de Negocios de IBM Security, cada cliente u organización es susceptible de ser atacado y es necesario que, además de herramientas de protección y seguridad, se haga uso de herramientas de inteligencia que cubran de punta a punta la problemática de seguridad empresarial.

Hay que concebir la inteligencia como la capacidad de las herramientas de adaptarse a problemáticas nuevas, comenta Pavez.

Inteligencia de seguridad es un nuevo paradigma y forma de entender la computación. "No basta con decir que una organización tiene una red estable y dispositivos de seguridad sino que hay que ir a la siguiente etapa y eso -sin duda- depende del nivel de madurez de cada compañía".

Para comprobar los niveles de madurez en cuanto a seguridad, Pavez recomienda una revisión interna respecto a controles de seguridad a través de algunas normativas como: COBIT, ISO 27000, etc., desde donde se puede definir en dónde está la organización y hacia dónde quiere llegar.

La compañía debe estar preparada para eventuales ataques y dar continuidad a los servicios y el negocio con una actitud preventiva y revisar potenciales vulnerabilidades.

Las empresas deben integrar la seguridad desde la concepción de la estructura de negocio de la compañía e incorporar aplicaciones de seguridad que tengan inteligencia, comentó Pavez.

CONOCIMIENTOS TÉCNICOS + ESTRATEGIA = PLAN INTEGRAL

También se analizó las tendencias sobre el enfoque que las empresas usuarias y proveedoras de productos de seguridad dan a este tema.

Juan Rivera, director para Cono Sur de Check Point, señaló que el negocio de la seguridad cambió de un enfoque tecnológico hacia una estrategia unificada para luego hacer la implementación de productos.

Cuando se genera una estrategia de seguridad unificada, dice el ejecutivo de Check Point, se da una reacción proactiva con la predisposición de anticipar potenciales problemas para la organización. Además, para Rivera, los fabricantes también están cambiando y re-educando a los consumidores y usuarios, de manera en que la seguridad sea tratada holísticamente y para ello sugiere acciones simples como la de "complementar los conocimientos técnicos con la estrategia".

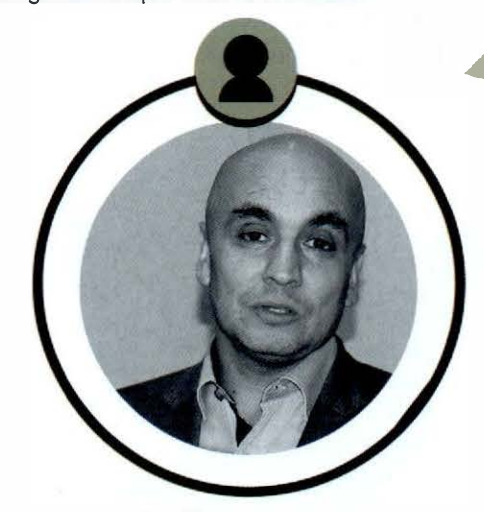
"El técnico debe seguir trabajando en su área pero a la vez aprender habilidades en el manejo de tácticas de inteligencia y ciberguerra, ya que un hacker piensa distinto a un ingeniero".

Rivera señala algunas recomendaciones sobre cómo un gerente de TI debería diseñar una estrategia y el proceso sería el siguiente:

1. Ver el escenario completo
2. Generar trabajo en conjunto con distintas áreas: finanzas, comercial...
3. Definir una estrategia de ataque externo e interno

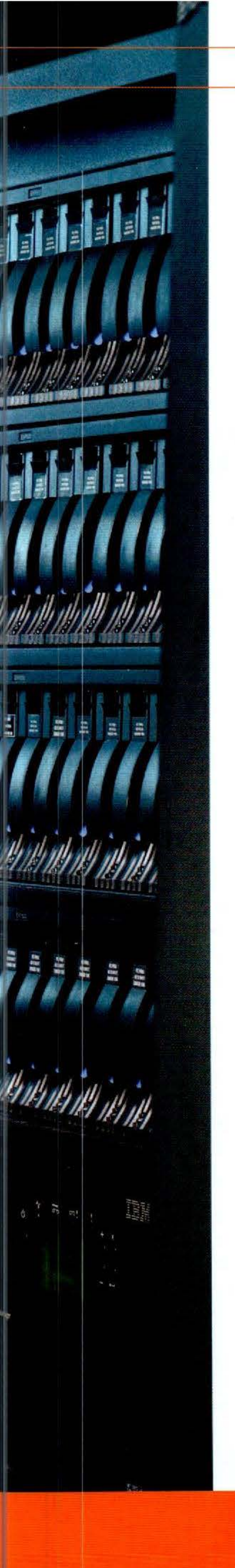
AMENAZAS DE PRÓXIMA GENERACIÓN

Bruno Sánchez, jefe Regional de GMS, dio a conocer las características más comunes de los atacantes para reconocerlos fácilmente; y, las herramientas que garantizan una seguridad y administración óptima para proteger la información de esas amenazas. Sánchez señaló que en Ecuador el número de ataques por malware (tipo de software que tiene como objetivo infiltrarse o dañar una computadora), ha sufrido un incremento acelerado en los últimos años. Así por ejemplo, Pichincha registra el mayor número de ataques a nivel nacional con un 69%, seguida por Guayas con 24%, y provincias como Manabí, Azuay, Tungurahua, Los Ríos, Loja, Esmeraldas, El Oro e Imbabura también aparecen en la tabla con pequeños porcentajes de ataques. Igualmente, la evolución de troyanos para móviles aumentó de 100 ataques registrados en 2012 a 3.000 en el 2014, por ello se recalcó la importancia de estar siempre protegidos.


Juan Rivera,
director para Cono Sur de Check Point



RUBÉN RECALDE • CIO PRONACA



"Hay que ser más para servir mejor a los demás"

RUBÉN RECALDE NO TEME QUE LE DIGAN "NERD" POR SUS AFICIONES Y SU TRABAJO, SIN EMBARGO, ESE CALIFICATIVO NO DESCARTA SU CARISMA Y SU VOCACIÓN POR SERVIR Y SER RECÍPROCO CON LA VIDA.

Rubén Recalde es el Director de Tecnología de Pronaca; tiene a su cargo un departamento compuesto de cinco gerencias y 60 ingenieros y su misión es liderar y gestionar los recursos tecnológicos necesarios para apoyar el negocio.

En su oficina, su escritorio está ordenado y despejado. Quien lo ve podría pensar que quien trabaja allí está de vacaciones. Sin embargo, es uno de los signos de que Rubén es metódico y organizado. Cada objeto tiene un lugar adecuado y las tareas por hacer van de izquierda a derecha. Así concibe "su línea de producción", como la llama. Es un hombre pegado a la fe del razonamiento, la lógica y el conocimiento pero también la convivencia en reciprocidad entre seres humanos.

Sus actividades profesionales empezaron como ingeniero de soporte para el área bancaria en Unisys, compañía norteamericana de tecnología de información que proveía entornos de misión crítica, sin embargo, su interés por el sistema operativo de los equipos lo llevaron a aprender más allá de la automatización del sistema operativo, lenguajes de programación y base de datos relacionales.

Con esas habilidades adquiridas a base de dedicación, curiosidad y aprendizaje natural, Recalde obtuvo fortalezas de hardware, software y de transmisión de datos.

Fue un niño dedicado a los estudios. Sonríe espontáneamente cuando habla de sus calificaciones y no teme en señalar que toda la vida fue un "nerd". Estudió en el Colegio Montúfar donde fue abanderado, y más tarde en la Escuela Politécnica del Ejército, también obtuvo altas calificaciones.

El contacto con los clientes como ingeniero de soporte le indicó el camino a seguir a Recalde. Se dio cuenta que el pensamiento lógico de un ingeniero debía complementarse con un pensamiento estratégico que aporte a la línea estratégica del negocio.

Su matrimonio y la firme idea de crecer laboralmente le impulsan a buscar nuevas opciones. Aplicó en Xerox para un cargo afín a ventas, pero luego de la entrevista de trabajo afinó su visión de corto plazo y las ventas no eran

HITOS:

1990

Fue uno de los primeros de su promoción en graduarse como ingeniero electrónico en la Politécnica del Ejército

1992

Es el año que consta en sus registros laborales como ingeniero de soporte en Unisys

1996

Gerente de Tecnología de Ecuatoriana de Aviación

1998

Jefe de Soporte de Pronaca

2005

Gerente de TI de Pronaca

POSICIÓN ACTUAL:

Director de Tecnología de Pronaca





RETOS:

Involucrar los negocios de la organización con conceptos de tecnología.



IMPLEMENTACIONES IMPORTANTES:

- Apoyo a implementación primer ERP
- Manejar toda la operación de tecno logia bajo estándares internacionales
- SOA
- Data Center

su fortaleza, y allí definió cómo quería verse profesionalmente y su visión era la de llegar a ser un alto ejecutivo que forme parte de la estrategia de una compañía.

Ingresó a Comlasa, empresa dedicada a proveer en Latinoamérica servicios tecnológicos para aerolíneas, y se especializó en telecomunicaciones con lo que reforzó sus conocimientos sobre esta área y trabajó con protocolos distintos de transmisión, empaquetamiento de datos, etc.

Frente a la posibilidad de ocupar un cargo gerencial del área técnica fuera del país en una aerolínea norteamericana e ir sin su familia, decidió permanecer en el país y aplicar a una de las empresas más importantes del país. Ocupó el cargo de Jefe de Soporte en Pronaca y trabajó en la operatividad del departamento de tecnología, justo en el momento en que la compañía había definido implementar un ERP. Para esa época, la implementación de un ERP significaba marcar un hito tecnológico.

En estos 17 años en Pronaca, Recalde menciona importantes retos profesionales. Propuso gerenciar toda la operación de tecnología bajo estándares internacionales, además, incorporar SOA o Arquitectura Orientada a Objetos y reducir de 120 a 50 aplicaciones integradas bajo un bus de servicio empresarial o ESB. Convirtiendo a esta compañía en una de las primeras en implementación de esta arquitectura y, para complementar, inició la implementación del data center. De todos estos procesos, comenta Recalde, el reto personal más grande ha sido involucrar los negocios de la organización con conceptos de tecnología.

> "Ser más para servir mejor. Soy el principal servidor de los 60 ingenieros que me reportan".

Estudioso de la fe racional de los jesuitas, y gracias al involucramiento con grupos de profesionales de la Universidad Católica, está interesado en el análisis y la práctica de los Ejercicios Espirituales de San Ignacio de Loyola, a los que considera una guía de "couch" de 500 años. Recalde se apoya a nivel profesional y personal en ésos preceptos espirituales, de la ley de la cosecha y crecer para servir mejor. "Creo en que hay que ser más y no para uno mismo sino para servir mejor a los demás", y lo resume de esta manera "Yo soy el principal servidor para los 60 ingenieros que me reportan"

Este pensamiento se ha vuelto práctica. Comparte lo que conoce y sabe: tecnología, liderazgo y lo hace con el espíritu de devolver lo que ha recibido.

Rubén Recalde es un ejecutivo que forma parte de toda una estrategia organizacional y ya tiene una nueva meta: convertirse en vicepresidente de Desarrollo. Sabe que aún no está preparado pero lo hará con la misma dedicación y entusiasmo con que inició su carrera profesional.

Iniciativas que mueven el entorno del emprendimiento

La región tiene una nueva generación de líderes emergentes que encuentran su espacio de desarrollo en el mundo del emprendimiento y en particular del mundo digital, señaló Raúl Rivera, chileno, emprendedor y activista de la innovación, en su visita al país.

Las gacelas, como describe Rivera a la gente que innova de manera disruptiva, es una nueva generación de emprendedores que entiende que no pueden ser exitosos si solo se quedan en el "vecindario", para ello deben ser lo suficientemente buenos para competir.

Pero si las personas deben tener estas características, las empresas también deben cumplir mínimos requisitos para salir al mundo y es que deben ser dinámicas.

En la región existen experiencias interesantes, como el caso de TNX, una compañía tecnológica chilena que desarrolla e implementa soluciones y ha alcanzado un reconocimiento por Gartner como una de las compañías latinoamericanas líderes en la industria de las telecomunicaciones.

Al mencionar a Ecuador, Rivera señaló que Kruger Lab es una de las iniciativas donde se encuban cosas importantes gracias a gente con talento y muchas ganas. Sobre la región mencionó que América Latina tiene desafíos en temas de libre competencia y aranceles

En relación a la libre competencia, la lógica conductual de la región se ha caracterizado por la introducción de ideas de fuera adaptadas, o de la mano del estado capturando alguna área protegida por el mismo estado, o existe una tendencia a monopolizar ciertos sectores y disminuir el nivel de competencia.

Este modelo no es equivocado y se ha dado en todo el mundo, dice Rivera. Sin embargo, frente a una región que se caracteriza por prácticas anticompetitivas, ahora se agrupan para darle una voz a los emprendedores y corregir ciertas políticas públicas que perjudica a emprendedores más disruptivos e innovadores, indicó.

El emprendedor tiene su rol y es hacer bien las cosas y los innovadores por definición prueban y fallan y la razón porque son exitosos es porque prueban y fallan temprano y les sale barato, comenta Rivera.

Hay casos en que la gente persigue una idea sin cuestionarse permanentemente si hace lo correcto y cuando esto sucede viene el fracaso y les cuesta recuperarse, mientras que otros fallan permanentemente y continúan.

90%

DE LAS PYMES no llegan a los 10 años de existencia, debido a que la mayoría de las ideas no son buenas y si lo son no siempre consiguen el factor comercial. "Hay que entender que la innovación es un deporte de equipo y hay que tener uno equilibrado", según Raúl Rivera.

Espacios que apoyan emprendimientos

En el ecosistema del emprendimiento, se suman algunos mecanismos que aportan el proceso de emprendimientos, uno de ellos, son las áreas de co-working donde se crea un ambiente de colaboración y las condiciones necesarias para impulsar el establecimiento de negocios a partir de ideas.

La consultora de emprendimiento, innovación, y RSE Hélène Billaud, actualmente administra Buen Trip, un lugar de co-working, señala que este tipo de espacios aportan un ambiente inspirador y motivador para trabajar y conectarse, además, en el caso del ambiente que administra, existe la posibilidad de capacitación a través de cursos y talleres para aprender, eventos para conectarse entre profesionales y potenciales clientes, y una red de mentores para un proceso de pre incubación y acompañamiento de los emprendedores en etapa de desarrollo.

En estos espacios también se generan iniciativas que promueven la participación en actividades mundiales. Una de ellas, es el Space Apps Challenge que también se realizó en Quito y que reunió a desarrolladores, técnicos, ingenieros, diseñadores, programadores y entusiastas a resolver retos de relevancia global relacionados con la vida en la Tierra y el Espacio.

En esta hackaton participaron 32 talentosos, 8 mentores y hubo tres equipos ganadores del Space Apps Challenge Quito 2015 y fueron:

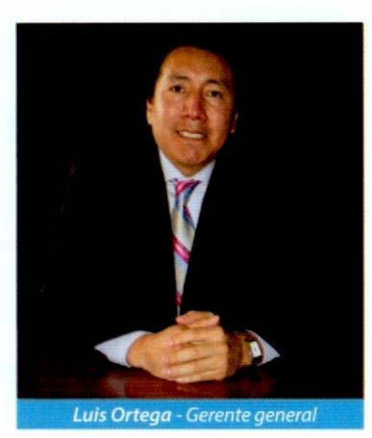
Raíz, una plataforma web para compartir conocimientos y experiencias sobre pestes, cultivos, plantas, pesticidas y también alertar sobre tendencias de problemas que están afectando al entorno.

Y Dropi Alone que desarrollaron una aplicación móvil para





Sinergy Team: Evolución y retos cumplidos


Luis Ortega - Gerente general

Sinergy Team es una empresa que nació hace 13 años con la visión de proveer soluciones tecnológicas innovadoras que se ajusten a las necesidades del mercado ecuatoriano. En sus inicios, el portafolio de productos a entregar era reducido, sin embargo, la adopción de tendencias tecnológicas en el país, los requerimientos de clientes así como la capacitación y conocimiento de nuevas herramientas impulsaron a que Sinergy Team amplíe su portafolio de soluciones tecnológicas.

En la actualidad Sinergy Team cuenta con soluciones de Nube e Infraestructura, Seguridad Inteligente, Optimización IT y Activos Eficientes.

Una fórmula para el éxito

Desde sus inicios, Sinergy Team ha cumplido un rol entre sus socios de negocios y clientes bajo una filosofía que se sustenta en cumplir la promesa al cliente, mediante atención, seguimiento, satisfacción y cumplimiento de las necesidades de sus clientes del sector público y privado.

A lo largo de estos 13 años, Sinergy Team ha logrado cumplir sus retos de posicionamiento de su nombre entre sus clientes, el reconocimiento de sus socios de negocios, así como un crecimiento sostenido. Su fórmula es sencilla: combinar conocimiento y experiencia del talento humano, sumado al potencial que significa generar, identificar y madurar oportunidades de negocio, un trabajo directo con clientes, y la ejecución coordinada dan como resultado proyectos exitosos, clientes satisfechos.

Pero los retos de Sinergy Team no tienen límites y menos aún fronteras. Bajo las mismas premisas y el modelo de trabajo y con la confianza y apoyo de IBM y Nexsys, sus principales socios de negocios, prevén la apertura de operaciones de negocio en Panamá y Bolivia.

Una fortaleza adicional de Sinergy Team es la gestión de su administración. Luis Ortega, actual gerente general, es uno de los fundadores de esta compañía ecuatoriana, su trayectoria, perfil profesional y expertise sobre la evolución de las tendencias tecnológicas y la adopción en el mercado ecuatoriano le otorgan a Sinergy Team un valor adicional de seguridad y confianza.

Premios y reconocimientos

El trabajo constante y la dedicación a los clientes tanto del área de tecnología como a sus directivos ha sido crucial en el crecimiento de Sinergy Team. Por ello ha recibido, de distintas categorías el reconocimiento de sus socios de negocios:

- ***2015:** Canal con mayores ventas Año 2014*
- ***2013:** Mejor canal de software en ventas Año 2012*
- ***2012:** Mejor Software IBM cuentas del mercado medio*
- ***2012:** Mejor Canal de Software IBM en el 2011*
- ***2009:** Mejor Business Partner Gestión Nexsys Latinoamérica*

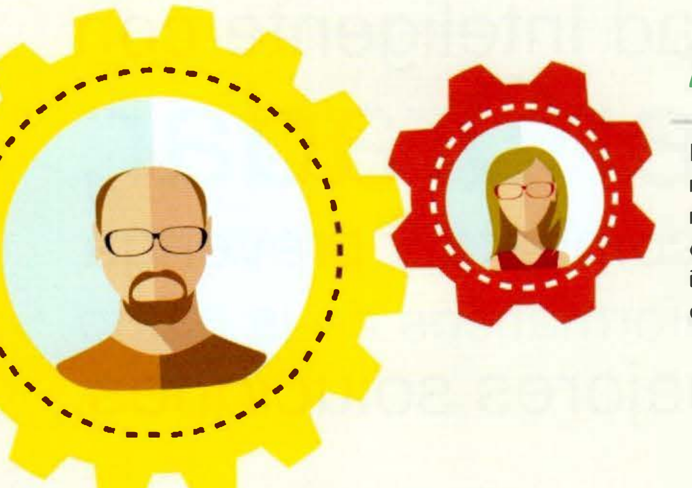
Casos exitosos de implementación

Banca: BNF, BIEES, Bco. del Pacífico, Bco. de Guayaquil, Bco. del Austro
Privadas: Corporación El Rosado; Telefónica, Ayasa,
Gobierno: Super. de Compañías, DINARDAP, Rio Napo, Transelectric





analizar el daño producido por ozono en hojas a través de tomar una fotografía de hojas y compartir los datos para ser analizados y publicados en un mapa colaborativo.
El equipo 3D Designed Medical Tools fue nominado en la categoría People Choice gracias al diseño de 4 herramientas de un kit médico con tecnología de impresión 3D para los astronautas.
Estas iniciativas aportan en el entorno de emprendimiento a ubicar talentos, mostrar los emprendedores locales, conectarse con otros ecosistemas y personas con similares intereses.
Héléne Billaud, dice que una startup como emprendimiento que empieza debe tener una respuesta rápida y eficaz a todas las situaciones nuevas que se presentan "es estar en constante habilidad de tomar rápidamente decisiones en situación de incertidumbre e ir construyendo una empresa"



Apoyo de las empresas de tecnología

En el ecosistema de emprendimiento las empresas tecnológicas tienen una tarea importante, y es el apoyo para crear laboratorios de innovación internos, patrocinar emprendimientos en sectores similares que aporten a su cadena de valor y a su productividad, y organizarse independientemente del estado para desarrollar sectores de innovación, finaliza Billaud

Emprendimientos internos

Las empresas de desarrollo han marcado el ritmo en materia de emprendimiento, gracias a acciones internas. Magmasoft, empresa ecuatoriana, dedicada al desarrollo de soluciones de negocio, estimula a sus colaboradores a poner en práctica sus ideas que luego se transformarán en productos y/o servicios empresariales complementarios para clientes, y lo hace a través de eventos internos en donde se dan a conocer las ideas de los colaboradores de la organización.
Ana Chaparro, gerente General de Magmasoft, comenta que las actividades internas permiten madurar las ideas de los colaboradores a través de conocimientos, mentoring o capital, además, tiene el objetivo de generar nuevos productos y servicios complementarios al portafolio existente.
La base de estas iniciativas es la confianza, dice Chaparro, y sobre todo el alinearse a elaborar ideas complementarias al portafolio de la compañía.
En este proceso participa una comisión liderada por el área de Investigación, Desarrollo e Innovación, que previamente revisa los proyectos basándose en 4 parámetros: innovación, viabilidad, sustentabilidad y la viabilidad comercial.
"Lo vemos como un reto muy interesante, sabemos los problemas que puede acarrear la incubación de nuevas empresas, sin embargo, creemos firmemente que los valores como la comunicación y la confianza es el éxito de este modelo de negocio", indica la ejecutiva de Magmasoft.



Aporte de las Startup al emprendimiento y desarrollo

- Las startups generan empleos calificados
- Forman a sus empleados para mayores niveles de rendimiento
- Adaptación y productividad.
- Ayudan a retener el talento ecuatoriano dentro del país
- Generan conocimientos tácitos


Presentes en:
Netsecure
— Quality IT Solutions —
Miami
Con más de 18 años de experiencia y una sólida estrategia para posicionarse en la región, Netsecure destaca entre los principales proveedores de tecnología, presentando un amplio portafolio en Soluciones de Seguridad.
Colombia
Ecuador
Perú
Chile
Argentina
Expertos en Seguridad Informática
Más información en: netsecure.com.ec

Los 10 datasets más RELEVANTES EN PROGRAMAS DE DATOS ABIERTOS

Por: Diego May
Co-fundador y CEO de Junar*

Con el objetivo de ayudar a las ciudades y agencias interesadas en implementar programas de datos abiertos se reseñan algunas sugerencias basadas en varias experiencias en Latinoamérica y Estados Unidos.

Para comenzar, es importante aclarar que la priorización de datasets varía de ciudad en ciudad y de agencia en agencia. Para poder definir realmente los top 10 datasets para las instituciones hay que tomar en cuenta lo siguiente:

1. REVISAR PEDIDOS DE INFORMACIÓN

Ciudades y agencias de gobierno reciben muchos pedidos de datos en forma constante. Se debe tomar en cuenta para definir los temas y para lograr hacer más eficientes estos procesos de entrega de información a la ciudadanía.

2. OBJETIVOS ESTRATÉGICOS DE LA AGENCIA

Las prioridades de un gobierno son una muy buena guía en la definición de qué sets de datos se deben abrir. Dependiendo de los objetivos, por ejemplo ser más eficientes, o más transparentes, o más innovadores, o reducir el crimen, o mejorar los sistemas educativos, la priorización de los datasets va a cambiar.

3. HABLAR CON LOS EXPERTOS EN EL MUNICIPIO

Los dueños y administradores de los datos conocen bien los datos existentes, sus fuentes y formatos, la utilidad de los mismos y cuál es la mejor manera de publicarlos para maximizar su entendimiento y uso. Es clave que estas personas sean parte de los equipos que definen las prioridades para el programa de datos abiertos.

Con estos tres puntos clave es posible definir un plan de datos abiertos sostenible y exitoso en el mediano y largo plazo y que a la vez esté alineado con los objetivos y recursos de la agencia o municipio.

A continuación se describe a grandes rasgos los sets de datos más populares:

PRESUPUESTO Y ASPECTOS FINANCIEROS EN GENERAL. Este es típicamente el primer eje temático a considerar. Probablemente la agencia ya publica algún reporte (no en formato de datos abiertos) y esto está definitivamente alineado con objetivos de transparencia. Tiene total sentido considerar este dataset para abrirlo de forma adecuada (y acceso a estos datos vía API por ejemplo).

1 ¡MAPAS/GIS/CARTOGRAFÍA!

Si le preguntan a la unidad de GIS de la agencia, ellos ya tienen mucha información y probablemente ya la estaban abriendo de una u otra manera. Los mapas son información muy útil y visual. A veces estos datos están abriéndose en formatos poco amigables para gente que no es experta en GIS. Es clave que el portal de datos abiertos incluya esta información y la haga fácil de ubicar, entendible y utilizable.

2 PERMISOS VARIOS

Este suele ser un dataset muy relevante. En el caso de municipios existen muchos permisos que se entregan diariamente. Tener acceso a ellos y al estado de los mismos a lo largo del proceso es muy útil y se han generado apps interesantes alrededor de estos datasets, como por ejemplo BuildingEye.

3 DATOS SOBRE PROYECTOS RELEVANTES

Con mucha frecuencia agencias/municipios lanzan proyectos importantes (nuevo estadio, centro de convenciones, mejoras al aeropuerto, un gran evento, programas de salud, etc.). Estos proyectos son de alto interés y probablemente involucrarán una partida de presupuesto substancial. Estos proyectos representan buenas oportunidades para apertura de datos y para generar mayor participación, transparencia, e innovación.

4 TRANSPORTE

La información relacionada con vehículos de transporte público, sus horarios y rutas hasta información que proveen los GPS para el rastreo de los vehículos son de interés para los municipios. Tener estos datos, sean estáticos, en tiempo real o de actualización diaria y no publicarlos sería un desperdicio.

5 DATOS DE PEDIDOS DE LA CIUDADANÍA

En Estados Unidos son los sistemas 311. En Latinoamérica tiene distintos nombres según diferentes regiones. Sea cual sea el nombre, abrir el dataset que muestra los pedidos de la ciudadanía y el estado de progreso de estos pedidos es relevante. Este set de datos en combinación con otros ha dado nacimiento a muchas aplicaciones.

6 PARQUES, RECREACIÓN Y TURISMO

Mapeo de parques, centros de recreación, puntos de turismo y hasta mapas de los árboles en una ciudad. Es amplia la diversidad de sets de datos que se pueden considerar en este eje temático. Para aquellas ciudades en que el turismo representa un componente importante en la ecuación de desarrollo económico, abrir estos datos es de alta prioridad. Información como la cantidad de hoteles, el tráfico, eventos, restaurantes o agenda cultural pueden generar alto valor y dar origen a aplicaciones interesantes.

7 INFRAESTRUCTURA DE LA CIUDAD

Datos acerca del estado de las calles y el pavimento, las autopistas, las rutas de los camiones de limpieza, o de otros aspectos y proyectos de infraestructura sueles ser de gran relevancia. Abrir los datos con los que se cuenta puede ser una rápida forma de generar tráfico al sitio, por parte de ciudadanos y de desarrolladores de software.

8 INFORMACIÓN DE ESTACIONAMIENTOS

Llegar al centro de la ciudad y saber dónde estacionar y poder pagar fácilmente es de valor para el ciudadano. Cuando las ciudades tienen sensores en parqueos y sistemas de parqueos, traer esos datos (idealmente en tiempo real) puede ser de alto valor y permite generación de apps.

9 MEDIO AMBIENTE Y SOSTENIBILIDAD

A través de ciudades con sensores de medición de ruido y polución. Datos relevantes y en tiempo real permiten la toma de decisiones a entidades de gobiernos locales para la aplicación de acciones de emergencia.

10 OTROS SETS DE DATOS

De iniciativas que incluye información relevantes de salud: hospitales, clínicas, número de pacientes, enfermedades, programas de vacunación; en educación: cantidad de escuelas, colegios y universidades, notas, graduados; de emergencias: centros de asistencia, programas, estadísticas, etc.

* Junar es una plataforma de datos abiertos

Nuevos actores bajo normativas y estándares para el aseguramiento de la Información



Asegurar los recursos tangibles e intangibles en una organización dejó de ser una frase de moda y se convierte poco a poco en una prioridad considerando el aumento de ataques y robos de información. Las buenas prácticas de gobierno corporativo, normativas y estándares internacionales, así como regulaciones y leyes puntuales para el caso del sistema financiero, por ejemplo, son la base para crear una cultura formal para asegurar la información. El sector privado bancario, comercial, industrial, telecomunicaciones han mantenido un interés por los temas de seguridad, sin embargo, desde hace 5 años, el Estado con la creación de la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación se suma a la tarea de adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información de las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.



Aplicación de normas internacionales

En Ecuador, se aplican normativas internacionales relacionadas con la Seguridad de la Información, entre ellas, el estándar internacional ISO/IEC 27000, en la versión del 2015 en los sistemas implementados antes del año 2013.

Katalina Correa, gerente de Certificación de Bureau Veritas, empresa con experiencia evaluando el cumplimiento de los clientes con normas y regulaciones relacionadas con la Calidad, Salud y Seguridad, Ambiente y Responsabilidad Social, señala que la información constituye un activo que, al igual que otros activos del negocio, es de gran valor para una empresa y necesita contar con medidas de seguridad adecuadas.

A nivel de empresas privadas es común que se alineen a determinados estándares y normativas que les permitan establecer una hoja de ruta para aplicar políticas y controles de seguridad. En muchos casos, las empresas implementan estándares aunque no se certifican. Por ejemplo, las normas ISO son aplicables en el país a todas las organizaciones que tienen activos y sistemas de información. Correa acota que aunque reciben requerimientos por parte de clientes, sin embargo, son muy pocas las empresas que se han certificado y las que lo hacen pertenecen al sector bancario y de telecomunicaciones.

Para implementar una certificación es necesario un proceso previo que va desde la capacitación del personal a la implementación de un Sistema de Gestión para luego rea-



Sector financiero: Seguridad sustentada en la administración del riesgo operativo

Uno de los sectores que mayor regulación ha tenido en materia de seguridad ha sido el financiero a través de la Ley General de Instituciones del Sistema Financiero que señala entre otras que las instituciones del sistema financiero cuenten con fuertes medidas de seguridad en la tecnología de información y comunicaciones a fin de que los elementos tecnológicos utilizados para entregar sus productos y/o servicios sean seguros y confiables; la necesidad de contar con los controles necesarios para proteger los intereses del público.

La regulación sobre todo está sustentada en el riesgo operativo en el que se pueden dar acciones de "fraude interno" y "fraude externo", ocasionados por el uso inseguro de la tecnología de información y comunicaciones.



lizar auditorías necesarias y, finalmente certificar.

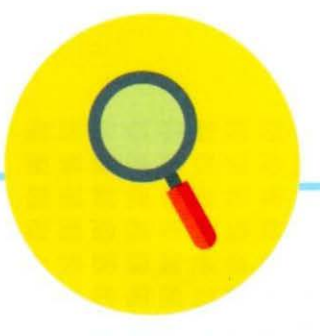
Las certificaciones en materia de seguridad benefician a las empresas pues permiten contar con una guía adaptable según las características y tipo de empresas.

Para tomar medidas de seguridad adecuadas, es necesario una correcta identificación y clasificación de la información, y una sistemática evaluación de riesgos por amenazas y vulnerabilidades que se pueden dar en las empresas.

Existen normas como la norma internacional ISO 27001 que pone de manifiesto los requisitos relacionados con los Sistemas de Gestión de Seguridad de la Información, como un recurso que permite a las organizaciones la evaluación de riesgos y la implementación de medidas de control para mantener la confidencialidad, integridad y disponibilidad de los activos de información. El objetivo fundamental, indica Correa, consiste en proteger la información de la organización para que no llegue a manos equivocadas o se pierda para siempre.







El Acuerdo 166: un marco referencial para las instituciones del Estado

Desde el 2011, el Estado Ecuatoriano, a través de la Secretaria Nacional de la Administración Pública, SNAP, creó la Comisión para la Seguridad Informática y de las Tecnologias de la Información y Comunicación para establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional.

En el 2013, emitió un acuerdo ministerial que señala el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información a todas las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

El Acuerdo 166, vigente desde septiembre del 2013, posibilita a través de la implementación del Esquema Gubernamental de Seguridad de la Información, EGSI, un marco referencial para implementación de controles de seguridad.

El EGSI se basa en 715 controles y su aplicación en dos fases. En la primera, se debe cumplir con 126 controles prioritarios obligatorios divididos por dominio de seguridad según la ISO27000, y que en el caso de la EGSI se relacionan con: Politicas de Seguridad de Información; Organización de la Seguridad, Gestión de los Activos de Información, Seguridad de Recursos Humanos, Seguridad Fisica del Entorno, Gestión en Comunicaciones y Operaciones, Control de Acceso, Adquisición y Mantenimiento de Sistemas de Información, Gestión de Incidentes de la Seguridad Informática, Gestión de Continuidad del Negocio y el Cumplimiento.

Desde la Subsecretaria de Gobierno Electrónico, se quiere dar un impulso al EGSI. Christian Chicaiza, director Nacional de Arquitectura Seguridad y Redes de la Secretaria Nacional de la Administración Pública, señala que posiblemente no sea necesario obligar a implementar los 126 controles de la primera fase sino que a partir del análisis de los activos críticos definir controles y el tipo de seguridad que requiere cada institución.

"En la implementación de controles de seguridades en un sistema de gestión de seguridades de la información, lo primordial es la identificación de los activos criticos de la organización", comenta Chicaiza.

Cumplimiento del EGSI en el 64.3%

En el cumplimiento de los 126 hitos de seguridad al 25 de marzo del 2015 están 81 instituciones, que corresponde, al 64.3% del total de las 129 entidades públicas registradas en el ranking de cumplimiento de la implementación; además, entre el 90 y 100% de cumplimiento del Esquema Gubernamental de Seguridades de la Información según los hitos seleccionados están ya el 39% de instituciones.

Lo que se ha logrado con la aplicación del Acuerdo 166 es contar con un marco de referencia inicial en temas de seguridad de información que permita conocer el nivel de madurez de cada institución e identificar sus fortalezas para ir más allá a un comité de seguridad gubernamental, indicó el ejecutivo de la SNAP.



DINARDAP es una de las primeras en cumplimiento del EGSI

Solamente la Dirección Nacional de Registro de Datos Públicos, DINARDAP, cumplió al 100% con los requerimientos de la primera y segunda fase del EGSI.

Dos años antes del acuerdo 166, la DINARDAP, debido a su eje de acción y a sus objetivos de establecer los mecanismos de regulación y de intercambio de información con las entidades que poseen registros de datos públicos, implementó normativas y estándares de seguridad basados en el standard ISO27000 con un enfoque en el modelo de gestión de defensa en profundidad.

En este proceso se identificaron, clasificaron y realizaron análisis de riesgo de los activos críticos y cuando debieron aplicar el acuerdo 166 la tarea fue más sencilla.

Uno de los primeros requerimientos del EGSI para todas las instituciones se refería a la incorporación del Oficial de Seguridad de la Información, el responsable de seguridad del área Informática y la conformación del Comité de Seguridad.

En la DINARDAP, el Oficial de Seguridad coordinó acciones siguiendo la estructura organizacional, así en el caso de esta institución se trabajó coordinadamente con el director de Protección de la Información, y con la parte jurídica.

En este organismo estatal existe una diferenciación dentro de la Coordinación de Infraestructura y Seguridad de la Información, la dirección de tecnología abarca todo lo relacionado con tecnologia, mientras que la dirección de seguridad todo lo relacionado con este tema. Sin embargo, tanto la parte normativa, marcos regulatorios, procesos y procedimientos se conjugaban con la parte tecnológica, es decir la dirección de Seguridad de Informática es transversal a todos los procesos.

Habilidades que marcan diferencias

Con el Acuerdo 166 en marcha, se ha evidenciado aún más, las diferencias de las áreas de Seguridad de la Información y Seguridad Informática, y también el perfil de los profesionales que asumen el cargo como Oficial de Seguridad.

Para Katalina Correa, gerente de Certificación de Bureau Veritas, la Seguridad Informática hace referencia a temas de Tecnología exclusivamente, es decir, Sistemas de Información, infraestructura de TI, mientras que la Seguridad de la Información es un concepto mucho más amplio que define la información como un activo que tiene valor para las organizaciones incluyendo las personas, los datos, la reputación, infraestructura y por supuesto los activos de TI.

Mauricio Vemaza, gerente Comercial de Sinergy Hard, empresa consultora de Tecnología, indica que la Seguridad de la Información y Seguridad Informática están ligadas en la práctica y no solo se requiere establecer políticas de seguridad sino además, implementar herramientas adecuadas que faciliten el control de las políticas.

Con esta diferenciación, el Oficial de Seguridad tiene habilidades que no son necesariamente técnicas sino relacionadas con: Conocimiento de normativas y estándares de seguridad, Sistemas de Gestión de Seguridad y el conocimiento del negocio y el funcionamiento de sus procesos.

De la experiencia de José Luis Barzallo, especializado en Derecho y Tecnología, a nivel empresarial, es relativo quien debe ser el responsable de seguridad, sin embargo, quien ocupe esta posición deberá estar a nivel del directorio de la empresa ya que las buenas prácticas corporativas señalan que debe estar a un nivel decisor o gerencial.

En la mayoría de los casos, aún forma parte del área de sistemas o tecnología, muchas veces está a cargo del gerente de TI, y su nivel de jerarquía depende del organigrama interno de la empresa.

Y Vemaza coincide y señala que a nivel empresarial el tema de seguridad debe estar alineado con la alta gerencia para alcanzar resultados óptimos.



A continuación Mauricio Vemaza, de SinergyHard, recomienda a los CIO o ejecutivos a cargo de la seguridad lo siguiente:

- Los encargados de seguridad deben comunicar eficientemente a nivel interno y abrir compromisos para implementar planes de seguridad.
- Definir el estado de madurez de las compañías para establecer niveles de seguridad
- Hacer un análisis para definir la brecha de lo que existe a la proyección de un estado óptimo
- Adquirir las habilidades necesarias para interpretar la información que le provee las herramientas implementadas
- Capacitación y formación adicional en estándares como: Sistemas de Gestión de Seguridad de Información, normas como la 3066, ISO27000.
- Involucrar a las distintas áreas del negocio para definir, clasificar la información crítica, activos y los privilegios de acceso, etc.
- Finalmente, adquirir herramientas necesarias para cumplir con las políticas de seguridad definidas

CERTIFICACIONES DE SEGURIDAD PARA PROFESIONALES

- Auditor líder con la norma ISO/IEC 27000
- Certi ied Ethical Hacking (CEH)
- Information Systems Security Professional (CISSP)
- Certi ied In ormation Security Manager (CISM)



Análisis y seguimiento de leyes sobre seguridad

José Luis Barzallo, abogado especializado en Derecho y Tecnología, señala que temas como Seguridad de Información e Informática se trata dentro de la Constitución. Lo relacionado con Seguridad Informática en el Código Orgánico Integral Penal, COIP, a modo de protección e infracción de los sistemas informáticos.
En cuanto a Seguridad de la Información y desde la parte legal se refiere a la protección de los datos. Se pueden proteger datos personales y desde la propiedad industrial los secretos industriales o comerciales.
Estos dos hacen un vínculo que se conecta con el COIP respecto del uso y manejo de la información porque no es solamente que rompa un sobre o robe una carpeta sino que cuando se habla de información o secreto industrial, comercial o dato personal éste puede estar en papel o en cualquier medio informático.
A nivel empresarial, la seguridad de información sigue políticas internas, estándares internacionales en función del segmento al que pertenece cada empresa.
En las empresas a nivel privado, dice el especialista, la aplicación de estándares y normas ISO están implícitas y si un gerente o administrador no las cumple, los resultados que arroje su administración estarán sujetos al cumplimiento y seguimiento de este tipo de normas privadas.
Pero en el caso de tecnología hay algo adicional, comenta, y es que hay una responsabilidad que incluso podría caer en un delito por una omisión, es decir por incumplimiento.
Aunque no es un delito en sí mismo pero, si una empresa sufre un rompimiento de seguridades, el director de TI o gerente, o responsable de seguridad son los primeros sospechosos pues no aplicaron las normas.

El principio de neutralidad tecnológica

Para el sistema financiero, la Seguridad de la Información no entra en detalles tecnológicos como un principio de aplicación general porque habla del principio de neutralidad tecnológico y lo que efectivamente se da son pautas de aplicación para prevenir riesgos en las instituciones financieras.
La empresa privada tomará parámetros para aplicarlos proporcionalmente siguiendo un análisis que definan los recursos tecnológicos a implementar.
En un banco, es importante que se haga una inversión considerable pensando en que hay fondos que son del público y que deben ser protegidos, menciona José Luis Barzallo, especialista en Derecho y Tecnología.

Responsabilidades civiles y penales

Un gerente de TI o de seguridad es quien toma y aplica todas las normas de Seguridad de la Información de la organización y, si se dan robos de información en el sistema, según las condiciones legales pueden establecerse procesos judiciales, indica Barzallo. El proceso se inicia con una investigación. Hay que estar conscientes de que, a pesar de tomar y hacer seguimiento a las políticas de la organización, es posible que sucedan fallas humanas y tecnológicas.

En lo legal, no se puede sancionar una conducta si la ley no la califica como delito, y bien puede aplicarse al ámbito de la Seguridad de la Información, así, si no hay normativas de seguridad, políticas, disposiciones legales no se puede cometer delito. Barzallo menciona a modo de sugerencia que para la aplicabilidad de la seguridad debe colocar en el tope de la pirámide a las buenas prácticas internacionales que son recomendaciones; a las políticas internas y finalmente, la parte legal.

NORMA 27001

ISO 27001 Sistemas de Gestión de la Seguridad de la Información (SGSI). Es la norma que contiene los requisitos para que las empresas implementen y los entes certificadores auditen el Sistema de Gestión de Seguridad de la Información.

3S

Metodología de las 3S para aplicar normativas de seguridad

Esta metodología de las 3S, Seguridad, Simple y Sencilla está basada en el principio de "divide y vencerás", comenta Nancy Velásquez, asesora de Seguridad de la Información. La metodología está compuesta de módulos o bloques, donde cada uno cubre un objetivo de control que comprende el proceso y las herramientas que permiten automatizar el objetivo de control, para obtener métricas que faciliten la gestión de seguridad.

La mejora en las empresas se consigue a partir de ir implementando de estos módulos que se van acoplando entre sí, hasta completar el mapa de riesgos. La estrategia de implementación es comenzar por los puntos críticos del mapa de riesgos, señala la asesora.

NORMA 27000

ISO 27000 contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman.

Nancy Velásquez, consultora de Seguridad, actualmente, las áreas con mayor regulación en el Ecuador son las instituciones públicas a través del Acuerdo 166, derivado de la norma internacional ISO/IEC 27001:005, y el área financiera, donde la Superintendencia de Bancos ha solicitado a las Instituciones Financieras implementar el SGSI según lo estipulado en la norma ISO/IEC 27001:2013

CONTROLES críticos de seguridad INFORMÁTICA

Recientemente, DigitalSecurity, empresa ecuatoriana que provee soluciones tecnológicas, dictó un taller donde se señalan 20 controles críticos de Seguridad Informática como un listado de acciones específicas de aseguramiento que pueden ser tomadas en cuenta para establecer buenas prácticas dentro de la organización, estas son:

1. Inventario de dispositivos autorizados y no autorizados
2. Inventario de software autorizado y no autorizado
3. Configuraciones seguras para hardware y software en dispositivos móviles, laptops, estaciones de trabajo, y servidores
4. Evaluación constante de vulnerabilidades y re ediación
5. Defensa contra malware
6. Seguridad de software aplicativo
7. Control de acceso inalámbrico
8. Capacidad de recuperación de datos
9. Habilidades de evaluación de seguridad y formación adecuada
10. Configuraciones seguras para dispositivos de red como firewall, routers, switches
11. Licitación y control de puertos de red, protocolos y servicios
12. Control de uso de privilegios administrativos
13. Defensa de perímetro
14. Mantenimiento, monitoreo, y análisis de logs de auditoría
15. Control de acceso basado en la necesidad de conocer
16. Control y monitoreo de cuentas
17. Protección de datos
18. Manejo y respuestas de incidentes
19. Ingeniería de redes seguras
20. Test de penetración y ejercicios de equipo rojo

DIRECTORIO DE SEGURIDAD

ADEXUS S.A.

NACIONALIDAD EMPRESA	Chile
PRODUCTOS DE SEGURIDAD	Tecnologías para protección de plataformas internas, dispositivos móviles y procesos de negocios. Adexus cuenta con el Security Operation Center.

CLADIRECT

NACIONALIDAD EMPRESA	Ecuador
PRODUCTOS DE SEGURIDAD	• Firewall de siguiente generación • Deep Packet Inspection (Allot) • Switching, Routing y Seguridad (Juniper) • Firewall UTM (Watchguard) • DDoS (Corero) • Proteccion DNS (Secure 64) • WiFi con seguridad (Aruba)

COMPUEQUIP DOS

NACIONALIDAD EMPRESA	Ecuador
PRODUCTOS DE SEGURIDAD	F5 ofrece soluciones de seguridad para aplicaciones web. El WAF de F5 es certificado por ICSA LABS y funciona sobre una plataforma de propósito específico tanto de hardware como de software. F5 Application Security Manager protege contra el top 10 de vulnerabilidades identificadas por OWASP y además cumple las normas PCI. F5 Advanced Firewall Manager protege la red. Así mismo es certificado por ICSA LABS como Firewall Perimetral. F5 entrega una solución completa desde capa 2 a capa 7. Se complementan a estas soluciones, servicios por suscripción de filtrado URL, reputación de IPs y soluciones anti fraude para transacciones por internet, tanto para el usuario como para la aplicación.

COMSTOR

NACIONALIDAD EMPRESA	Estados Unidos
PRODUCTOS DE SEGURIDAD	Soluciones de Tecnología de Seguridad Cisco: virtual, en la nube, dispositivos, módulos, software para routers y switches. También incluyen el firewall Cisco Adaptive Security Appliance (ASA), así como routers y switches seguros, dispositivos de seguridad en la web, dispositivos de seguridad de correo electrónico, seguridad como servicio, seguridad de terminales, clientes VPN, y una variedad de otros dispositivos y productos de seguridad.

DIGITAL SECURITY

NACIONALIDAD EMPRESA	Ecuador
PRODUCTOS DE SEGURIDAD	SIEM - HP ArcSight Aplicaciones de seguridad - HP Fortify Siguiente generación de Firewall - Palo Alto Networks Gestión de vulnerabilidades - Qualys Guard VM Cuplimiento de Políticas - Qualys Guard PC Fuzz Testing - Codenomicon Defensics Gestión de Identidad - Lieberman Software Patch Management - Secunia CSI Vulnerability Intelligence - Secunia VIM DataBase Firewall - Imperva DAM Web Application Firewall - Imperva FAM Advanced Malware Protection - FireEye DDoS Protection - Arbor Networks Gestión de dispositivos móviles - Mobile Iron Endpoint Security - Kaspersky IDS - Snort Monitoreo de Seguridad de Redes - Security Onion

ELIXIRCORP

NACIONALIDAD EMPRESA	Ecuador
PRODUCTOS DE SEGURIDAD	Seguridad Informática: hacking ético, computación forense, auditorías y políticas de seguridad, manejo de incidentes

ENERIT

NACIONALIDAD EMPRESA	Ecuador
PRODUCTOS DE SEGURIDAD	Avast, Comodo,MyDLP, Kerio Control, Druva inSync, Sysaid, Entensys, Kemp, Spamtitan, Cyber Patrol, GlobalSignridad, manejo de incidentes

ENLACE DIGITAL

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Antivirus: ESET; Doble Factor de Autenticación: ESA OTP ; Cifrado: Deslock ; Backup: Storagecraft; Firewall- Seguridad Perimetral: Gateprotect; Anti-malware mobiles: ESET

GENSYSTEMS S.A

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Antivirus, firewall, Administrador Unificado de Amenazas (UTM).Seguridad Perimetral Gateprotect; Anti-malware mobiles: ESET

GMS

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Antivirus Firewall Encriptación de la información SIEM Protección para APT Big Data

I-SEC ECUADOR
Information Security del Ecuador INC. S.A

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	CONSULTORÍA SEGURIDAD DE LA INFORMACIÓN • ISO 27001 SGSI -Sistema Gestión de Seguridad de Información • EGSI 27001 - Acuerdo 166 • ISO 22301 Continuidad de Negocio & Recuperación Desastre TI • Gestión de Riesgos Seguridad de Información ISO 27005 • Ethical Hacking , Forense Informática • PETI- Planificación Estratégica TI
	CAPACITACIÓN • Líder Auditor ISO 27001 / Implementador ISO 27001 • Implementador Continuidad de Negocio BCP ISO 22301 • Seguridad de Información: ISO 27001, ISO 27002 • Gestión de Riesgos ISO 31000 , ISO 27005 • Ethical Hacking, Forense Informática • PETI - Plan estratégico de TI • COBIT, ITIL, Gestión por Procesos, Gestión de Proyectos

INNOVASYS

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Splunk

LOCKNETEC

NACIONALIDAD EMPRESA	**Colombia**
PRODUCTOS DE SEGURIDAD	Consultoría en Seguridad

NETSECURE

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Antivirus, firewall, encriptación de la información, gestión de incidentes, seguridad de identidades, SOC, análisis de vulnerabilidades, cifrado, etc

NEXSYS

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	PALO ALTO: Firewall, gestión para dispositivos móviles, IPS INTEL SECURITY: Antivirus, firewall, correlecionador de evento, DLP, IPS, encriptación de las conexiones, firewall de siguiente generación Symantec: Antivirus, antispam, DLP, Cifrado de archivos y correo, certificados digitales. Dell:Firewall IBM: Firewall, IPS, encriptación de la BD, seguridad en teléfonos

ROOT SECURE

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Análisis de Seguridad (Ethical Hacking) Análisis de Riesgos Charlas de Concienciación a Usuarios Asesoramiento en Seguridad de la Información Capacitación In Company Acompañamiento en la Certificación ISO 27001 SOC, análisis de vulnerabilidades, cifrado, etc



SATELITE.COM

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	PRODUCTOS SEGURIDAD Respaldo información (Backup, netbackup, máquinas virtuales) Encripción de datos Prevención de fuga de información - DLP Protección puntos finales, Filtrado de Contenido, Monitoreo Redes Virtualización Forense Informática / Respuesta a Incidentes
	CONSULTORÍA • Ethical Hacking • Implementación ISO 27001 (SGSI, EGSI) • Análisis Riesgos • Planes Continuidad de Negocio & Recuperación Desastre • Análisis Forense Informático.

SECURITY DATA

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Certificados de firma electrónica para personas naturales y jurídicas, certificados de servidor Seguro, correo firmado y encriptado, custodia gigital, facturación electrónica, Tokens, desarrollo de aplicativos de firma electrónica, desmaterialización de documentos

SINERGY HARD CIA. LTDA

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Inteligencia y Análisis de Seguridad, Gestión de Identidades y Accesos, Monitoreo y seguridad de las bases de datos, encriptación y enmascaramiento de datos, escaneo de vulnerabilidades, seguridad perimetral y de los puntos finales, seguridad de dispositivos moviles, GRC (gobierno, riesgo y cumplimiento), fraude electrónico, respaldo de la información, monitoreo, manejo de incidentes.firma electrónica, desmaterialización de documentos

SINERGY TEAM

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Firewall de base de datos Encriptación de base de datos Enmascaramiento de datos Gestión de identidad Gestión de usuarios privilegiados Protección de aplicaciones Web Protección de plataforma SOA Protección de puntos finales Protección de red Inteligencia de Seguridad

TECNOAV

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Monitoreo de logs, correlacionador de eventos, Firewalls UTM, Almacenamiento EMC, Gestión de identidades y Gestión de contraseñas usuarios privilegiados

TELALCA S.A

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Soluciones en seguridad de datos y seguridad perimetral, somos Fortinet en Ecuador

VIRTUAL IT

NACIONALIDAD EMPRESA	**Ecuador**
PRODUCTOS DE SEGURIDAD	Netsec

VU SECURITY

NACIONALIDAD EMPRESA	**Argentina**
PRODUCTOS DE SEGURIDAD	Dispositivos móviles y hardware de seguridad (Mobile Tokens), Análisis de fraude, reconocimiento de voz, billetera inteligente

25. WATCHGUARD

NACIONALIDAD EMPRESA	**Estados Unidos**
PRODUCTOS DE SEGURIDAD	Seguridad de Redes

LA SEGURIDAD de la Información es un compromiso

Germán Pancho

*Director de Maestría de Gerencia de Sistemas y Tecnologías de Información UDLA

La Seguridad de la Información no solo es una cuestión de las empresas, sino también de los individuos. En un entorno hiperconectado, las estrategias de protección deben tener su propia adaptabilidad a fin de que las amenazas y vulnerabilidades sean tratadas como un objetivo móvil.

La convergencia de las tecnologías de movilidad, nube, lo social y analítica; la redefinición constante de lo que se entiende como infraestructura crítica, las nuevas regulaciones de estados y organismos y la velocidad con la que se debe actuar para enfrentar estos retos han determinado que los programas de Seguridad de la Información, por una parte, sean más complejos y difíciles; y, por otra, en un aspecto que las empresas no pueden ignorar.
La gestión de un programa de seguridad de la información es una disciplina asociada al diseño, implementación y control de prácticas para salvaguardar los activos tecnológicos y procesos de negocio esenciales a lo largo de la empresa, cuyo despliegue no es homogéneo. La caracterización de su aplicación debe alinear la política de seguridad y los controles basados en riesgos con las necesidades organizacionales y la clarificación de responsabilidades a todo nivel.

En la gestión de función de seguridad de información, confluyen factores de naturaleza y complejidad diversa que deben ser tratados de forma sistémica para asegurar un tratamiento efectivo de las amenazas y los escenarios de negocio cambiantes. Esto explica el aparecimiento de dos nuevos conceptos: la arquitectura de seguridad empresarial y la seguridad inteligente.

En este escenario, el perfil de responsable de seguridad de la información, exige una integración de competencias técnicas y de negocio, con habilidades de creatividad y de visión; que permita hacer de la gestión de la seguridad de la información algo factible, considerando que la defensa o protección perfecta es un ideal y que, por tanto, es indispensable el desarrollo de las capacidades de detección, correlación e integración de información y, cuando sea necesario, de intervención y remediación, efectivas y eficientes.

La visibilidad del denominado Oficial de Seguridad de la Información, su autonomía y su ámbito de acción dependen del tamaño de la empresa, del giro de negocio y de la cobertura del impacto de las tecnologías de información. No existe una regla única. En empresas grandes y medianas, el Oficial de Seguridad podría liderar toda un área que involucre procesos de gobierno, planificación, arquitectura, despliegue de controles, evaluación de riesgos y de protección. En cambio en empresas pequeñas, el proceso que se privilegia es el de protección; este rol podría estar inmerso como parte de las funciones del departamento de TI. Sin embargo, en cualquier escenario, es recomendable definir, formalizar y desplegar un catálogo de procesos asociados a los temas de seguridad, con asignación de responsabilidades y recursos que lo soporten.

Para finalizar, es claro que la seguridad de la información se ha transformado en un compromiso y desafío global que requiere cambios culturales y que involucra a los proveedores de tecnología, a los gobiernos, a las empresas y a los consumidores.



Realizamos una breve encuesta, al finalizar dos eventos de seguridad, para conocer la opinión de Directores de Tecnología, Jefes de Seguridad, Gestores de Información, y encargados de Seguridad de la Información sobre inversión y prioridades en materia de seguridad.

Para no repetir cada uno de los 10 enunciados de la pregunta dos, solamente se puso la letra correspondiente a cada una de las opciones y el valor que fue asignado por las personas que respondieron.

1 ¿Cuánto prevé invertir en seguridad en 2015, frente al 2014?

a.- NADA
b.- IGUAL
c.- MENOS
d.- MAYOR

2 ¿Cuáles son sus prioridades de seguridad considerando que 1 es de menor valor y 10 el mayor valor?

a.- Cumplimiento regulatorio y conocimiento de políticas de seguridad
b.- Gestión de incidentes
c.- Infraestructura y recursos tecnológicos para paquetes de seguridad básico (antivirus, anti-spam, perímetro, endpoints)
d.- Seguridad electrónica (video alarmas, cámaras, reconocimiento facial, etc)
e.- Seguridad Factura y Firma Electrónica
f.- Fraude Online (transferencias bancarias, ventas con tarjetas de crédito, compras online)
g.- Protección de información de dispositivos móviles, aplicaciones y navegadores
h.- Encriptación de información
i.- Seguridad en nube
j.- Otros



JUAN PABLO ALIAGA
Independiente

1. MAYOR

2.
a.- 9	f.- 10
b.- 7	g.- 8
c.- 5	h.-8
d.- 5	i.- 6
e.- 8	j.- 0



DIEGO CASTILLO
Técnico Informática de Seguridad de la Información
Operaciones Río Napo

1. MAYOR

2.
a.- 10	f.- 1
b.- 10	g.- 7
c.- 8	h.-6
d.- 10	i.- 1
e.- 7	j.- 0



DIEGO CEVALLOS
Jefe de Seguridad
Cooperativa Cooprogreso

1. MENOS

2.
a.- 3	f.- 8
b.- 8	g.- 8
c.- 5	h.-8
d.- 2	i.- 8
e.- 2	j.- 1



DANIEL CHINCHÍN
Responsable Ciberseguridad
Armada del Ecuador

1. MAYOR

2.
a.- 1	f.- 1
b.- 6	g.- 1
c.- 8	h.-8
d.- 1	i.- 6
e.- 1	j.- 1



GRACE CORNEJO
Gerente de Seguridad Informática
Junta de Beneficencia del Guayaquil

1. MAYOR

2.
a.- 10	f.- 6
b.- 9	g.- 6
c.- 10	h.-6
d.- 2	i.- 7
e.- 10	j.- 1



HERNÁN ESTRELLA
Jefe de Tecnología
KUBIEC

1. MENOS

2.
a.- 2	f.- 2
b.- 2	g.- 6
c.- 9	h.- 5
d.- 6	i.- 5
e.- 10	j.- 0



FRANKLIN GARCÍA
Coordinador Nacional de Tecnología
IESS

1. MAYOR

2.
a.- 10	f.- 8
b.- 10	g.- 8
c.- 10	h.-10
d.- 9	i.- 8
e.- 10	j.- 0



RAMIRO GAVILANES
Gerente de Tecnología
PACO

1. MAYOR

2.
a.- 8	f.- 10
b.- 9	g.- 7
c.- 8	h.-7
d.- 7	i.- 6
e.- 9	j.-0





GALO IDROVO
Gestor de Información
Diners Club

1. IGUAL

2. a.- 10 b.- 10 c.- 5 d.- 5 e.- 5 f.- 10 g.- 8 h.-10 i.-8 j-5



MAX HINOSTROZA
Jefe de Seguridad Informática
Banco Nacional de Fomento

1. MAYOR

2. a.- 10 b.- 7 c.- 10 d.- 2 e.- 8 f.- 2 g.- 2 h.-8 i.- 1 j.- 0



WILSON MURILLO
Analista de Seguridad
Andes Petroleum

1. IGUAL

2. a.- 5 b.- 7 c.- 7 d.- 1 e.- 7 f.- 1 g.- 5 h.-5 i.- 1 j.- 0



CARLOS RAMÍREZ
Jefe de Seguridad de la Información y PMI
Automotores y Anexos

1. MENOS

2. a.- 1 b.- 5 c.- 10 d.- 1 e.- 1 f.- 5 g.- 5 h.- 1 i.- 1 j.- 10



RAMIRO SALAZAR
Responsable de Seguridad de la Informática
Banco Central del Ecuador

1. MAYOR

2. a.- 10 b.- 10 c.- 8 d.- 7 e.- 6 f.- 10 g.- 8 h.-10 i.- 1 j.- 0



JORGE SUÁREZ
Auditor Informático
Cooperativa Andalucía

1. MAYOR

2. a.- 10 b.- 7 c.- 8 d.- 7 e.- 10 f.- 8 g.-6 h.-10 i.- 1 j.- 0



MARY VARGAS
Independiente

1. IGUAL

2. a.- 10 b.- 10 c.- 10 d.- 1 e.- 5 f.- 7 g.- 1 h.-7 i.- 5 j.- 1



LUIS VILLARROEL
Director de Tecnología
YANBAL

1. IGUAL

2. a.- 10 b.- 10 c.- 8 d.- 10 e.-10 f.- 1 g.- 5 h.-5 i.- 10 j.- 0

Para disfrutar de Star Wars

Lego dispone de una amplia gama de productos de la película La Guerra de las Galaxias.
La nave Slave es un modelo exclusivo LEGO Star Wars. La Slave cuenta con cabina y alas giratorias con modos de vuelo y aterrizaje, además de cañones dobles y blásteres ocultos para defenderte de los ataques. Recrea la captura de Han Solo en el episodio V de Star Wars: El Imperio Contraataca y despega de Bespin con el héroe rebelde atrapado en carbonita en la bodega de carga. Puedes acoplar el soporte para colocar esta emblemática nave en su caracteristica posición de vuelo. Incluye 4 minifiguras con armas: Boba Fett, un guardia de Bespin, un soldado de asalto y Han Solo.





Una app para búsquedas laborales

Multitrabajos.com cuenta con la única aplicación de búsqueda de empleo para móviles en el Ecuador, teniendo en cuenta que la nueva generación de trabajadores hace uso intensivo de estos dispositivos. La aplicación permite al usuario acceder a todas las ofertas laborales del portal, seguir sus postulaciones, actualizar su CV y, sobre todo, tomar ventaja al competir más rápido por una vacante.
"Hasta la fecha, nuestra aplicación tiene más de 100.000 descargas en el Ecuador. Las proyecciones son muy favorables para el uso de dispositivos móviles en el país gracias a su penetración en todos los estratos sociales, así como el crecimiento de los jóvenes postulantes de la generación "Y"", dijo Néstor Milano, gerente General de Multitrabajos.com en Ecuador.

A poner en práctica sus ideas tridimensionales

Kikai Labs, fabricante argentino de impresoras 3D en serie, presentó su nuevo modelo M11 de impresora 3D perteneciente a la línea Fabber.
Esta impresora de tipo FDM (Fused Deposition Modeling) está construida en chapa de metal y acero inoxidable, con una cubierta externa de aluminio y cuenta con tecnología de auto-nivelación por medio de un sensor capacitivo industrial.
Posee una pantalla táctil color de 3.2". Por intermedio de esta pantalla, el equipo puede ser utilizado sin la necesidad de estar conectado a una PC, aunque también cuenta con un conector USB.



Smart MFP de Lexmark

El Ecosistema Inteligente y Simple

Conecte papel e información digital estructurada y no estructurada, con dispositivos y conexiones que impulsan sus negocios.

INTELIGENTE

Mejore el funcionamiento de tareas y procesos cotidianos

- Facilidad de uso • Desempeño
- Calidad • Cumplimiento

SIMPLE

Administre un entorno técnico y de negocios en constante cambio

- Flexibilidad • Gestión
- Seguridad • Servicios



